Alberta

PUBLIC WORKS SUPPLY AND SERVICES

SECURITY OF PERSONAL COMPUTER SYSTEMS

SYSTEMS MANAGEMENT AND COORDINATION BRANCH

COMPUTER SYSTEMS DIVISION

INFORMATION SERVICES

PUB. PWSS 152

April 1986

TABLE OF CONTENTS

	Page
1.0 INTRODUCTION.....	1
2.0 PROTECTING THE PC EQUIPMENT.....	3
3.0 PROTECTING DATA.....	5
4.0 PROTECTING APPLICATIONS.....	8
5.0 PROTECTING OTHER EDP ASSETS ACCESSED THROUGH COMMUNICATIONS....	12
Appendix A	
Appendix B	

1.0 INTRODUCTION

1.1 Purpose

The wide use of personal computers (PC) and general access to telecommunication links, while providing many benefits, may introduce serious potential security risks. To ensure effective protection of these valuable resources, managers, system designers and users must be aware of the vulnerabilities which exist and control measures which should be applied.

The intended audience of this document are managers and users of PC's. Generally, the term PC refers to single-user systems. However, a great deal of information covered here applies equally to other types of micro-processor based systems designed for use in a general office environment (e.g., word processors, work stations, and various types of office computer systems).

The objectives of this document are to provide both managers and users of PC's with an understanding of the information security threats involved in using such systems and approaches to reducing the associated risks.

1.2 An Aporoach to PC Systems Security

A systematic approach to identify and implement security requirements includes the following activities:

a) Identifying the information and other assets that require protection.

b) Identifying and evaluating the threats, specific vulnerabilities, and degree of exposure (risk) to information assets.

c) Selecting control measures which provide cost effective reduction of exposure.

d) On-going activities to review the continued effectiveness and appropriateness of controls.

For a single PC application, a less formal, qualitative analysis might well be sufficient. However, for applications involving multiple PC's, networking, etc., a rigorous analysis is needed.

1.0 INTRODUCTION (cont'd)

1.3 Organization of Material

The assets which require protection and the hazards to be avoided are tabulated below:

ASSETS	HAZARDS
PC Equipment	Theft, damage, destruction, misuse
Data	Modification, destruction, disclosure
Applications	Tampering, interference
Other EDP assets accessed through communications, e.g., other computers, applications and their data	Failures, errors, malicious acts of PC users

Sections 2 through 5 of this document discuss specific protection requirements in the following areas:

- o Protecting the PC Equipment
- o Protecting Data
- o Protecting Applications
- o Protecting Other EDP Assets Accessed Through Communications

In addition, a general action plan for implementing an information security program is presented in Appendix A. Appendix B contains a guide to security products for PC's.

2.0 PROTECTING THE PC EQUIPMENT

This section describes control measures to provide a safe physical environment for personal computer equipment.

2.1 Theft and Damage Protection

2.1.1 Generally, PC's should be placed in areas which have basic physical access controls (e.g., locks on the doors and people present during working hours).

2.1.2 In situations where it is not feasible to secure an entire area, the equipment can be placed in special workstation enclosures which may be closed and locked when the equipment is not in use.

2.1.3 To prevent theft of PC's, several types of equipment lockdown devices are available. They may be used to secure the equipment to a table or other fixed object. Some devices also prevent access to system power switch and, thus can help prevent unauthorized use of equipment.

2.1.4 Many systems contain valuable expansion boards (e.g., additional memory, modems, graphics, interfaces, etc). To protect against theft of such components, devices are available for some systems which simply lock the equipment cover.

2.2 Environmental Controls

2.2.1 The typical PC is sensitive to the quality of its electrical power source. It is considered useful to maintain PC equipment on a power source separate from appliances or office equipment.

2.2.2 PC's are low power devices. They generate less heat than a light bulb. Extensive fire detection and suppression devices need to be considered only if the value of the equipment, data and other items in the area is significant.

2.2.3 To protect PC equipment from possible water leaks, consideration should be given to inexpensive plastic equipment covers.

2.2.4 If portable systems are being used, care should be taken to avoid drastic changes in temperature or humidity (e.g., transporting a system from outside into an office). Before operation, sufficient time should be allowed for the equipment to adjust to the new environment.

2.0 PROTECTING THE PC EQUIPMENT (cont'd)

2.2 Environmental Controls (cont'd)

2.2.5 Static electrical charges can build up in personnel, especially if carpeting is used. A discharge can occur when the person touches the PC equipment. Such a discharge could cause damage to integrated circuit components or semiconductor memory. This problem could be minimized through the use of anti-static sprays, carpets or pads.

2.3 Magnetic Media Protection

2.3.1 Proper handling techniques for flexible disks should be well known to all users. General precautions include:

- o Always store in the protective jacket.
- o Protect from bending or similar damage.
- o Insert carefully into the drive mechanism.
- o Maintain an acceptable temperature range (50-125F).
- o Avoid direct contact with magnetic fields.
- o Do not write directly on diskette jacket or sleeve.

2.3.2 Exposure to ordinary contaminants (smoke, coffee, doughnut crumbs, etc.) is probably the major reason for failures in magnetic media. Therefore, particular care should be exercised to minimize such exposures.

2.3.3 Simple wear is another cause of failures. Therefore, it is important that backup copies be made of all important disks. Indeed, day to day operation should be conducted with a back up copy, and not the master copy of such diskettes. (Care should be exercised in ensuring that the licensing agreement of proprietary software is adhered to.)

3.0 PROTECTING DATA

Data must be protected from unauthorized or unintended modification, destruction or disclosure. The expected rate of problems vary with the nature of the media on which data is stored. This section describes appropriate control measures.

3.1 Primary Storage

Data in primary storage can be destroyed by a power loss, power surge, or even a jolt of static electricity. The best protection against data destruction is to keep copies. Thus data in primary storage should be periodically saved on secondary storage.

If the local power supply quality is unusually poor (e.g. large fluctuations in voltage or frequency, voltage spikes or frequent outages), then more extensive power conditioning, battery backup or uninterruptible power supply (UPS) system should be considered.

3.2 Removable Media

Data recorded on diskette are usually protected from disclosure by removing the diskette from the computer and storing it in a safe place, as though the data were on paper.

Data stored on diskettes or other removable media may be protected from modification and destruction by the preparation of backup copies. It is often easier to make a backup copy of the entire volume (e.g., diskette) after each use or at the end of the day if a given volume is used frequently during the day. (The issues discussed in (3.3.5) and (3.3.6) - cryptography and data residue - should be reviewed in the event the diskettes are shared with other users.)

3.3 Non-Removable Media

Data on a fixed file must be protected from accidental erasure, from failure of the device that would make it unrecoverable, and from disclosure.

3.3.1 Data on a fixed file are protected from erasure by making copies. The usual practice is for the copy to be placed on a diskette.

3.3.2 Copies on diskette are also the usual form of protection against the failure of the device itself. This is usually done by storing on a diskette with scheduled frequency those data sets that have been opened for writing since the last scheduled backup. This capability is usually provided by the operating system. The frequency of backup is selected

3.3 Non-Removable Media (cont'd)

so as to balance the time required for the backup against the updates that could be lost.

3.3.3 For systems that are connected to other systems, consideration should be given to the use of those other systems for the storage of backup copies of files (e.g., uploading a file).

3.3.4 If equipment must be shared by several users and cannot be monitored at all times, then logical access controls should be considered to protect data from disclosure. Examples of such controls are:

- o The owners of the data should specify which users are authorized to access which system resources (normally programs or data).
- o The user identification mechanism for PC's should require an identifier and an authentication code.
- o A procedure should be established which requires each user to perform a "system reset" before leaving the PC equipment. This will cause reinvocation of the log-on process.
- o The operating system is modified to cause a system reset after a predetermined period of system inactivity.
- o The operating system is modified so that all file open requests are intercepted to check for proper authorization.

3.3.5 Logical access controls covered above prevent unauthorized persons from gaining access to confidential data. Another approach to protect data from disclosure is to deny effective use of information even if access is gained. This approach is based on the use of cryptographic controls.

Cryptography is the process of transforming information (clear text) into an unintelligible form (ciphertext) so that it may be sent over insecure channels. The transformation process is controlled by a data string ("key"). Anyone intercepting the ciphertext while it is in the insecure channel would require the appropriate key to decrypt (convert back to clear text) the information. The intended receiver is assumed to have that key.

3.0 PROTECTING DATA (cont'd)

3.3 Non-Removable Media (cont'd)

The use of cryptography can be both complex and expensive. As such, it should be used only for highly confidential information. Further information on this subject can be obtained from the Systems Management and Coordination Branch of Public Works, Supply & Services.

3.3.6 Data residue is data that is stored in areas of disk or memory which have been released for reuse. Such information often can be read by subsequent users. A common example of the disk residue problem is associated with the erasing of the disk files (e.g., with the ERASE command). This process usually results only in the setting of a "file deleted" indicator in the file directory, not the physical erasure or overwriting of the actual data. It is dangerous therefore, to pass files to other users on diskettes which contain "erased" files of sensitive data. The problem also exists for hard disks, since the data remains potentially accessible to subsequent users of the system. Users should also recognize that many common programs (word processors) create and delete "scratch" files which the user never uses. The files could contain sensitive information and are exposed to the same vulnerability.

This problem can be solved either by using a program to "purge" (ie: overwrite) all file data or through the use of degaussing equipment. The needed programs are relatively easy to write. If neither of these two options are available, then the user can

(a) use an overwrite utility,
(b) encrypt sensitive files, or
(c) do not share the system with other users.

4.0 PROTECTING APPLICATIONS

This section describes control measures to protect applications from external interference, contamination and lack of availability of data.

4.1 Formal Software Development

In situations where important functions are being performed on PC's, management should consider application of formal controls over software development, testing and data integrity.

4.2 Data Integrity Controls

Most generic software tools (e.g., spreadsheet and database management systems) do not provide built-in facilities for checking the integrity of input data. Therefore, it becomes the responsibility of the user to build in such checks. These should include data format and range checks and other redundant cross checks of results. Managers should require supporting information and evidence necessary to assure that calculations and other data handling operations have been performed properly.

4.3 Operational Controls

When a major data processing application is implemented on a PC, operational procedures should include:

- o Data preparation and input handling procedures
- o Program change procedures
- o Program execution procedures
- o Media (diskette or tape) procedures
- o Output handling and distribution procedures

These are, of course, the same type of procedures needed for large-scale system applications. It is important to recognize, however, that the personnel performing such procedures probably will not have extensive data processing or operations training and will be performing the duties along with their other responsibilities.

4.4 Isolation Controls

Applications on PC's must be protected from other applications running on the same system. Whenever two applications share storage, it is at least conceivable that an action of one will damage data belonging to the other. Computers that are intended for concurrent use by two or more users often implement isolation schemes to prevent this interference.

4.0 PROTECTING APPLICATIONS (cont'd)

4.4 Isolation Controls (cont'd)

Most systems that are intended for use by a single person at a time do not provide such process-to-process isolation. Such systems are not appropriate for groups of users who have a need to control data access among themselves, since any control mechanisms are likely to be ineffective.

In a system that is intended for use by a single person, isolation can be maintained by placing programs and data for different applications on separate diskettes.

4.5 Placement of Audit Trails

Designers of important applications will require reliable audit trails. The types of event that may be of interest include:

- o System startup
- o User session initiation and completion
- o Program initiations and completion
- o Access to certain files

Audit trail information can be recorded as part of an access control process. However, designers should avoid dependence on the PC to provide a safe environment for the storage of such data. It may be too easy for a user to modify or delete such data. If it is important enough to keep audit trail information on the PC, the system should be provided with appropriate physical and access control safeguards to protect the integrity of that data. If access to a host system is involved, the host is the proper location for the placement of audit data capture mechanisms.

4.6 Contingency Planning

Contingency plans should consist of emergency procedures, resources (hardware, software, data, etc.) backup preparations, and backup operation plans. In addition, comprehensive contingency plans will include recovery and test procedures. This sub-section will focus primarily on the first three areas.

4.6.1 Emergency Procedures

Any area in which people work and important information is handled should have basic emergency procedures including:

4.0 PROTECTING APPLICATIONS (cont'd)

4.6.1 Emergency Procedures (cont'd)

- o Alarm activation and deactivation procedures
- o Evacuation plans
- o System shutdown procedures
- o Lockup procedures
- o Medical emergency supplies and procedures
- o Fire detection and extinguishing equipment
- o Bomb threat procedures

4.6.2 File Backup

The users of PC's should provide for regular and systematic backup of files. The method and frequency of backup must be determined by each user, based on the storage media and the volatility of the data involved.

Errors on backup copies can obviously have disasterous consequences. Most PC systems provide disk and file comparison programs. Assurance of successful backup can be achieved by performing file comparison of original and backup copies. Some operating systems provide a write-verification option which will read each disk record immediately after it is written to verify its accuracy. Most backup, file copy, or file comparison utilities will provide a display of files processed. This information should be directed to the printer and stored with the backup media.

The obvious reason for file backup is to enable recovery of data after loss due to media or hardware problems or accidents. To provide for timely recovery, users store backup copies in a convenient nearby location. There is always the possibility of data loss resulting from a fire, theft, or other event which might involve an entire office or building. Appropriate protection measures against such threats require storing periodic archival copies at a remote location.

4.6.3 Other Backup Considerations

Data files are not the only things that can be lost, damaged or destroyed. Indeed, without the necessary equipment, personnel, and documentation, the data files themselves may be useless. Therefore, users must identify all elements which comprise their PC applications.

4.0 PROTECTING APPLICATIONS (cont'd)

4.6.3 Other Backup Considerations (cont'd)

- One advantage of widespread use of PC's is built-in equipment backup. However, not all systems are compatible. Different equipment options, installation variations, and privacy protection mechanisms used in many popular software packages can make "portability" extremely difficult. Therefore, advanced planning is critical.

- Application software backup consideration may differ depending upon the source of the application software.

For locally developed or maintained applications, backup should include source program files and optionally, loadable versions of all software. The required computer or interpreter programs should, of course, also be backed up.

Applications on PC's are often built around mass marketed "generic software". Much of this software is distributed with privacy protection mechanisms that link the software to a given machine or "system" disk. This may cause considerable difficulties when trying to conduct backup operations on different equipment or with alternate versions of the software.

The operation of PC applications often require a detailed knowledge of procedures which may not be documented. If such applications have any long term value, it should be clear that their operation should not be dependent on a single person. In emergency situations, others should be able to understand and use the applications. This requires specific efforts to document procedures and perhaps, cross-train personnel.

5.0 PROTECTING OTHER EDP ASSETS ACCESSED THROUGH COMMUNICATIONS

Increasingly, there is a need to connect PC's as terminal devices to larger host systems or to connect two or more PC's in network. Appropriate security issues of interest to management are covered here.

5.1 The Micro As An Accomplice

The danger posed to host systems due to increasing availablity of PC's (i.e., the potential of the PC as an "accomplice") has received considerable attention in the news and entertainment media.

Although there is certainly some reason for concern, it is important to recognize that almost no new host system security threats result directly from the use of PC's. The PC is functionally the same type of threat as a "dumb" terminal, and adequate security measures for terminal access have been available for a long time. Some of the security measures provided by the host are:

- o Each authorized individual is provided with a unique identifier and a secret password.
- o Authorization to system resources is by means of a list or algorithm that associates the resources with the user identifier.
- o Administrative procedures for adding and deleting users and granting and revoking authority are both timely and consistent.

PC managers should familiarize themselves with the security provided by the host computers. Further, they should ensure compliance by the users.

5.2 Terminal Emulation

When a PC is used as a terminal device to a host system, the basic requirements for security and access control remain with the host as covered above. As far as the host is concerned, there is just another terminal out there.

It should be recognized, however, that the PC has the ability to upload and download larger amounts of data at rates exceeding those with ordinary terminals. The PC managers should review the adequacy of controls based on the amount and types of data downloaded or uploaded.

5.0 PROTECTING OTHER EDP ASSETS ACCESSED THROUGH COMMUNICATIONS (cont'd)

5.3 PC Networks

When two or more personal computers are connected in a network, communication security becomes a problem. It must be recognized that in most local area network (LAN) systems, all nodes have the ability to read all traffic on the network. Therefore, privacy cannot be assured without the use of cryptographic protection. Most commercially available data encryption devices will work with PC's as well as other devices. There are also available devices which are incorporated into the PC (expansion boards) which include complete communications and cryptographic protocol functions.

APPENDIX A

RECOMMENDED ACTION PLAN

A formal security management program is a key to providing consistent and effective controls. The following plan of action is recommended.

A. Establish an Information Security Policy

A formal information security policy is a pre-requisite to a workable security program. This requires, at a minimum:

- o Identifying the types of information requiring protection (e.g. personal, trade secret, etc.);
- o Emphasizing the use of risk management approach to make protection decisions;
- o Assigning responsibility (and necessary authority) for security to the actual "owners" and users of the information resources;
- o Ensuring that security requirements are specified in all procurements of systems and equipment;
- o Requiring establishment of formal plans and procedures to respond to emergency or disaster situations.

B. Develop an Inventory of Applications

For PC's, it is considered useful to start with each hardware system and document the following:

- o System identification, location
- o Responsible user (i.e. the "owner")
- o Other users
- o General categories of sensitive information handled
- o Specific, identifiable applications
- o General description of access controls and other security measures currently in place

C. Conduct a Risk Assessment

The concept of risk analysis and management are central to any rational information security programs. The purpose of risk analysis is to determine the exposure to loss for a given system. Risk management is concerned with reducing those risks to an acceptable level.

Except for the obvious need to provide physical protection for the equipment, the security concern should be with the application, not the equipment. If a system is not being used for sensitive or critical applications, then a formal (i.e. quantitative) risk analysis is not necessary. If, on the other hand, a highly sensitive or critical application is being run on the small system, then a detailed risk assessment must be performed regardless of the value of the computer equipment itself.

(For additional information on Risk Analysis, please contact the Systems Management and Coordination Branch of P.W.S.S.)

D. Select Control Measures

For those systems or applications for which risks are determined to be unacceptable, additional control measures must be implemented. In general, such controls fall into one of the following categories:

- o Physical protection
- o Administrative procedures
- o Self developed software
- o Commercial security products

Since the "basic" personal computer generally provides very little in the way of security mechanisms, it is the user's responsibility to provide whatever controls are deemed necessary.

E. Audit and Monitor the Results

After selecting and implementing appropriate security measures for PC systems, management should conduct a post-implementation review and subsequent periodic audits. This is needed to ensure that control measures are, indeed, in place and operational and that they remain appropriate as the organization and its information environment change.

APPENDIX B

SECURITY PRODUCTS

This appendix provides a list of the types of products that are commercially available which can provide additional protection in several areas.

A. Physical Access Control and Theft Protection

- o Lockable equipment enclosures and workstations
- o Equipment lockdown devices
- o Power switch locks
- o Equipment cabinet or enclosure locking devices
- o Equipment removal detection devices

B. Electrical Power Quality Control

- o Surge Suppressors
- o Power "Conditioning" Systems
- o Uninterruptable Power Supply (UPS) Systems

C. Environmental Protection

- o Fire detection and suppression equipment
- o Water detection alarms
- o Temperature and relative humidity monitors
- o Dust covers
- o Static mats, sprays, or grounding devices
- o Dust filters, fans, etc.

D. Magnetic Media Protection

- o Lockable storage devices
- o Colour coded labels and jackets
- o Protective containers and mailers
- o Degaussing and destruction equipment
- o File encryption systems

E. Systems and File Access Control

- o User authenticators
- o Card or badge readers
- o Authentication code devices
- o File access control systems
- o Port protection devices - devices which control remote access to a system

APPENDIX B (cont'd)

F. Cryptographic Systems (Features)

- o Hardware or software implementation of the cryptographic algorithm
- o Hardware or software implementation of supporting functions
- o Private or public key
- o Automatic or manual key generation, entry, storage, and distribution
- o Proprietary or public (e.g. DES) algorithms

G. Miscellaneous

- o System utilities - to enable use of write-protect, "hide" files, and other system facilities which can be used for additional protection

- o CRT privacy screens - covers for CRT screens which limit screen viewing to a narrow angle of view.

hb/0056A
0002A